# Selected Cybersecurity GRC Projects

## ISO 27001 Gap Assessment – Financial Services

* • Performed a full ISO 27001 readiness audit for a small financial services provider, covering 8 control domains.
* • Identified 18 key control gaps and developed a remediation roadmap aligned with Annex A and NIST CSF references.
* • Drafted foundational cybersecurity policies, including access control, asset management, and incident response.
* • Outcome: Client achieved Stage 1 audit clearance within 60 days of roadmap implementation.

## Third-Party Risk Framework – SaaS Startup

* • Designed a tailored third-party risk evaluation framework based on CIS Controls.
* • Assessed 7 cloud-based vendors for compliance posture, data protection measures, and supply chain security risks.
* • Produced risk scorecards and defined thresholds for risk acceptance and remediation.
* • Outcome: Guided client to reject two high-risk vendors, strengthening procurement due diligence.

## Security Governance – Telecom Equipment Integration

* • Oversaw secure integration practices during 5G and LTE rollout projects across 60+ cell sites.
* • Reviewed Change Requests and Scope of Work (SoW) documentation for security exposure and compliance alignment.
* • Established IAM baselines and secure configuration checklists in line with internal cybersecurity policy.
* • Outcome: Reduced misconfiguration and deployment risks across multiple integration activities.

## NIST CSF Maturity Assessment – Nonprofit Organization

* • Conducted a cybersecurity maturity assessment based on the NIST Cybersecurity Framework.
* • Assessed capabilities across Identify, Protect, Detect, Respond, and Recover functions.
* • Provided a targeted improvement plan and conducted security awareness training for non-technical staff.
* • Outcome: Increased security awareness score by 30% in post-training evaluations.